EXHIBIT C

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
1	**virtual private network (VPN)**	a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers	"Improvements to the basic design include … a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry …" Abstract. "Data security is usually tackled using some form of data encryption. An encryption key 48 is known at both the originating and terminating terminals 100 and 110. The keys may be private and public at the originating and destination terminals 100 and 110, respectively or they may be symmetrical keys (the same key is used by both parties to encrypt and decrypt). Many encryption methods are known and usable in this context." Col. 1:38- 45; see also col. 1:16-37. "Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or	"[A] VPN is simply defined as the 'emulation of a Wide Area Network (WAN) facility using IP facilities' (including the public Internet, or private IP backbones)." B. Gleeson et al., Request for Comments (RFC) 2764, A Framework for IP Based Virtual Private Networks (Feb. 2000) p. 4. "The key issue that separates WAN technologies from LAN technologies is scalability – a WAN must be able to grow as needed to connect many sites spread across large geographic distances, with many computers at each site." Douglas E. Comer, Computer Networks and Internets (2d ed. 1999) p. 168. "A Wide Area Network (WAN) can span sites in multiple cities, countries, or continents." Douglas E. Comer, Computer Networks and

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to maintain. They can be compromised by virtual machine applications ("applets"). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc." Col. 2:52-63. "Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over	Internets (2d ed. 1999) p. 167. Dr. Mark Jones, a professor of Electrical and Computer Engineering at Virginia Tech, may offer expert testimony regarding the view of one of ordinary skill in the art as of the filing date of the '135 patent. Additionally, the named inventors may offer testimony regarding the view of one of ordinary skill in the art as of the filing date of the '135 patent. The following is a brief description of the substance of Dr. Jones' and/or the named inventors' testimony about the term "virtual private network (VPN)": 1. what makes a virtual private network (VPN) "virtual", "private" and a "network";

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			the Internet without any compromise in security." Col. 5:8-12. "Further improvements described in this continuation-in-part application include: … a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry …" Col. 5:65-6:3. "FIG. 26 shows a system employing a DNS proxy server with transparent VPN creation." Col. 7:20-21; Fig. 26. FIG. 26 "FIG. 27 shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function." Col. 7:22-23; Fig. 27. FIG. 27	2. network characteristics and functions, including capability to expand and how computers communicate with each other in a network; 3. why a "virtual" network includes computers that communicate through paths between them over another network; 4. how paths between computers in a private network are secure; 5. how paths between computers in a non-private network may be insecure; and 6. how encryption can be used for secure communications between computers on paths that may not otherwise be secure or private.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			"Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security." Col. 11:39-43. "Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like." Col. 19:42:44. Col. 23:11-20. "A detailed example will now be provided with reference to FIG. 24. As shown in FIG. 24, a first computer 2401 communicates with a second computer 2402 through two routers 2403 and 2404. Each router is coupled to	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			the other router through three transmission links. As described above, these may be physically diverse links or logical links (including virtual private networks)." Col. 36:25-32. FIG. 24 "The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: … (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry …" Col. 32:29-36. "B. Use of a DNS Proxy to Transparently Create Virtual Private Networks A second improvement concerns	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function." Col. 37:19-21; also see col. 37:40-49. "This conventional scheme is shown in FIG. 25. A user's computer 2501 includes a client application 2504 (for example, a web browser) and an IP protocol stack 2505. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack 2505) to a DNS 2502 to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application 2504, which is then able to use the IP address to communicate with the host 2503 through separate transactions such as PAGE REQ and PAGE RESP." Col. 37:30-39.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			"One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535)." "The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users. According to certain	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user." Col. 37:59-38:2; see also 38:3-12. "FIG. 26 shows a system employing various principles summarized above. A user's computer 2601 includes a conventional client (e.g., a web browser) 2605 and an IP protocol stack 2606 that preferably operates in accordance with an IP hopping function 2607 as outlined above. A modified DNS server 2602 includes a conventional	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			DNS server function 2609 and a DNS proxy 2610. A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2704. An "unsecure" target site 2611 is also accessible via conventional IP protocols." Col. 38:13- 22. "According to one embodiment, DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			virtual private network be created between user computer 2601 and secure target site 2604." Col. 38:23-33. "Some or all of the security functions can be embedded in gatekeeper 2603, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy 2610 communicates with gatekeeper 2603 to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site. Various scenarios for implementing these features are described by way of example below: Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN." Col. 39:34-52. "Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would reject the request, informing DNS proxy server 2610 that it was unable to	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			find the target computer. The DNS proxy 2610 would then return a "host unknown" error message to the client." Col. 39:53-60. Col. 1:38-45; 19:42-44; 37:30-32; 38:14-16; 38:66-39:25. "VPN Virtual Private Network, a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted." Glossary for the Linux FreeS/WAN project, p. 24 (submitted with Paper No. 10 (Supplemental IDS), dated February 22, 2002)) (VNET00221226, VNET00221418).	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			"FIG. 2C is a generalized diagram of a typical network." U.S. Patent No. 6,332,158 (Risley et al.) (cited in the '135 patent, see Paper No. 10, p. 5 (VNET00221088)); Risley '158, Fig. 2C; see also col. 5:62. FIG. 2C "It is currently state of the art of the Internet to create Virtual Private Networks (VPNs) using Internet Protocol Security (IPSec). However, there exists no standard nor current implementation for configuring and implementing the connection of systems in this Internet environment, such as between systems using the Transmission Control Protocol/Internet Protocol (TCPIP) and systems using the Internet Protocol Security (IPSec)." U.S. Patent No.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			6,330,562 (Boden et al.), col. 1:28-31 (cited in the '135 patent, see Paper No. 10, p. 4 (VNET00221087)). VNET 00221857 ("new locations" can be "easily added to the network"). VNET 00221135 (col. 7:44-49). "With the onset of network computing came the need to insure secure connections between networked computers. Usually companies resorted to establishing private networks to do this, and at considerable expense. However, as this trend of Network Computing continues to evolve, it is necessary to extend secure communications within the enterprise and to utilize the public networks. Driving factors include the need for	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			mobility, company mergers and acquisitions, and the usual 'improving the bottom line'. Virtual Private Networks (VPNs), in this context, allow customers to use existing private or public networks, including the Internet, to establish secure connections between other businesses, branch offices, and remote users." Boden '562, col. 1:41- 53. Cf. U.S. Patent No. 7,010,604.	
2	**Domain Name Service (DNS)**	a lookup service that returns an IP address for a requested domain name	See Intrinsic Evidence for "VPN" above and "DNS proxy server" below. In addition: "FIG. 25 shows a conventional domain-name look-up service." Col. 7:18-19; Fig. 25. FIG. 25 (PRIOR ART)	See Extrinsic Evidence for "domain name." "Domain Name System: Abbreviated DNS. 1. A system used on the Internet to map the easily remembered names of host computers (domain names) to their respective Internet Protocol (IP) numbers. 2. A software database program that converts domain names to Internet Protocol addresses, and vice versa."

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			"Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser and then used by the browser to contact the destination web site." Col. 37:22-29 "This conventional scheme is shown in FIG. 25. A user's computer 2501 includes a client application 2504 (for example, a web browser) and an IP protocol stack 2505. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack 2505)	McGraw- Hill Dictionary of Scientific and Technical Terms (6th ed. 2003) p. 638. "Domain Name System: Abbreviated DNS. 1. A system used on the Internet to map the easily remembered names of host computers (domain names) to their respective Internet Protocol (IP) numbers. 2. A software database program that converts domain names to Internet Protocol addresses, and vice versa." McGraw- Hill Dictionary of Electrical & Computer Engineering (2003) p. 172. "Domain Name Service (DNS): In Internet, a program that keeps track of the alphabetic names of other machines and their corresponding numeric IP addresses. The *Domain Name Service* translates a request to a named machine into the

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			to a DNS 2502 to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application 2504, which is then able to use the IP address to communicate with the host 2503 through separate transactions such as PAGE REQ and PAGE RESP." Col. 37:30-39. "In the conventional architecture shown in FIG. 25, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web	numeric IP address necessary to make the connection." Frank Hargrave, *Hargrave's Communications Dictionary* (IEEE Press, 2001) p. 168. "DNS: An abbreviation of Domain Name Service. A TCP/IP protocol for collecting and maintaining network resource information that is distributed among various servers on the network. It includes a method of translating network host names into network addresses; that is, it can provide a machine's IP address if given the machine's domain names." Frank Hargrave, *Hargrave's Communications Dictionary* (IEEE Press, 2001) p. 167. "DNS: Abbreviation of Domain Name System, or Domain Name Service. Over the Internet, a system which translates a domain name,

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet." Col. 37:40-49. "One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535)." Col. 37:50-58. "The conventional scheme suffers	such as www.yipeeee.com, into an IP address, such as 91.2.133.206." Steven M. Kaplan, *Wiley Electrical and Electronics Engineering Dictionary* (IEEE Press, 2004) p. 206. "Domain Name Service: On an Internet-connected computer, the software program that translates the domain name into the Internet Protocol (IP) address using a Domain Name Server." Jonar C. Nader, *Prentice Hall's Illustrated Dictionary of Computing* (3d. ed. 1998) p. 194. "**DNS**… *n.* **1.** Acronym for **D**omain **N**ame **S**ystem. The system by which hosts on the Internet have both domain name addresses (such as bluestem.prairienet.org) and IP addresses (such as 192.17.3.4). The domain name address is used by human users and is automatically

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users." Col. 37:59-62. Col. 38:43-52; 39:21-25; 39:53-60. "Domain Name Service, a distributed database through which names are associated with numeric addresses and other information in the Internet Protocol suite." Glossary for the Linux FreeS/WAN project, p. 9 (submitted with Paper No. 10 (Supplemental IDS), dated February 22, 2002)). "The Domain Name System (DNS) is an integral part of the Internet and other networks that use Internet-type protocols (such as TCP/IP) and architecture	translated into the numerical IP address, which is used by the packet-routing software. *See also* domain name address, IP address. **2.** Acronym for **D**omain **N**ame **S**ervice. The Internet utility that implements the Domain Name System (see definition 1). DNS servers, also called *name servers*, maintain databases containing the addresses and are accessed transparently to the user." Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 155. "**DNS server**… *n.* A computer that can answer Domain Name Service (DNS) queries. The DNS server keeps a database of hose computers and their corresponding IP addresses. Presented with the name apex.com, for example, the DNS server would return the IP address of the hypothetical company Apex. *See also* DNS (definition 2), IP

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			similar to the Internet. DNS allows human users to access information on different computers connected to the Internet by typing, entering, selecting or otherwise specifying, text names as opposed to sequences of numbers. This makes it much easier to remember, access and convey the location of information in the vast Internet. For example, "coolsite.com" is generally more appealing to the average user of the Internet than '199.227.249.232.'" U.S. Patent No. 6,332,158 (Risley et al.), Col. 1:40-50; 1:53-67 (cited in the '135 patent, see Paper No. 10, p. 5 (VNET00221088)). "FIG. 1A illustrates a DNS lookup as performed in the prior art; FIG. 1B illustrates the prior art's handling of valid and invalid	address. Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 155. The following is a brief description of the substance of Dr. Jones' and/or the named inventors' testimony about the term "Domain Name Service (DNS)": 1. how a Domain Name Service (DNS) is used in the Internet or World Wide Web; 2. characteristics and functionality of different types of DNS, including DNS according to the IETF RFCs; 3. examples of requests made to a DNS; and 4. examples of different responses a DNS may provide.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			domain name queries." Risley '158, col. 5:53-57. FIG. 1A PRIOR ART "FIG. 1A illustrates a DNS lookup, also called a "mapping" or "resolving" of a domain name to a machine address, as performed in the prior art. In FIG. 1A, computer 10 makes a request of computer 12. Computer 12 forms part of the Internet and, in particular, is a name server within the DNS. For example the request from computer 10 may come from a Web browser application executing on computer 10. In response to computer 10's user typing in a domain name such as www.bessemer_ventures.com, resolver code used by the browser transmits the domain name query to computer 12. This assumes that computer 12 has been	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			predesignated as the primary domain name server for computer 10. Computer 12 includes DNS name server software that receives the request. One method of DNS lookup allows computer 12 to check a local list of domain names already matched to machine addresses. If the queried domain name is in the local list then computer 12 can respond with an answer, in the form of the associated machine address, immediately. Such a local list is referred to as a "name cache" that is stored in system random access memory (RAM), disk storage or other storage associated with computer 12. The name cache is updated periodically from other, authoritative, name servers in the Internet.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			Assuming computer 12 does not have a match for the queried domain name in computer 12's name cache, computer 12 begins a process of querying other name servers in the Internet, such as computers 14, 16 and 18, for knowledge of the associated machine address. This querying is organized but takes time because of the limitations of the Internet and the ever-increasing number of domain name queries that need to be handled by a limited number of name servers. For a detailed discussion of DNS lookup, see the above reference. After computer 12 has obtained the machine address associated with the domain name www.bessemer_ventures.com, the machine address, 180.201.15.250, in this case, is passed back to computer 10 as the answer to computer 10's domain name	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			query." Risley '158, col. 2:4-41. "FIG. 1B illustrates the prior art's handling of valid and invalid domain name queries." Risley '158, col. 3:38- 39. FIG. 1B PRIOR ART Compare VNET 00221403 (FreeS/WAN definition of a "DNS"). Compare '135 patent, claims, 2, 3, 4, 5 and 8.	
3	**domain name** (including domain)	a name corresponding to an IP address	See Intrinsic Evidence for "DNS proxy server" below and "DNS" above.	"The naming scheme used in the Internet is called the *Domain Name System (DNS)*. Syntactically, each computer name consists of a sequence of alpha-numeric segments separated by periods." Douglas E. Comer, *Computer Networks and Internets* (2d ed. 1999) p. 366. "Domain Address: an Internet address in conveniently readable

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
				form, such as jones.com, as opposed to the IP address, which consists of numbers." Dictionary of Computer and Internet Terms (Barron's, 6th ed. 1998) p. 137. "An alphanumeric string which identifies a particular computer or a network on the Internet." McGraw-Hill Dictionary of Scientific and Technical Terms (6th ed. 2003) p. 638. "An alphanumeric string which identifies a particular computer or a network on the Internet." McGraw-Hill Dictionary of Electrical & Computer Engineering (2003) p. 172. "**DNS**… *n.* **1.** Acronym for **D**omain **N**ame **S**ystem. The system by which hosts on the Internet have both domain name addresses (such as bluestem.prairienet.org) and IP

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
				addresses (such as 192.17.3.4). The domain name address is used by human users and is automatically translated into the numerical IP address, which is used by the packet-routing software. *See also* domain name address, IP address. **2.** Acronym for **D**omain **N**ame **S**ervice. The Internet utility that implements the Domain Name System (see definition 1). DNS servers, also called *name servers*, maintain databases containing the addresses and are accessed transparently to the user." Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 155. "**domain**…*n.* **1.** In database design and management, the set of valid values for a given attribute. For example, the domain for the attribute AREA-CODE might be the list of all valid three-digit numeric telephone area codes in the

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
				United States. *See also* attribute (definition 1). **2.** For Windows NT Advanced Server, a collection of computers that share a common domain database and security policy. Each domain has a unique name. **3.** In the Internet and other networks, the highest subdivision of a domain name in a network address, which identifies the type of entity owning the address (for example, .com for commercial users or .edu for educational institutions) or the geographical location of the address (for example, .fr for France or .sg for Singapore). The domain is the last part of the address (for example, www.acm.org). *See also* domain name." Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 158. "**domain name**… *n.* An address of a network connection that identifies the owner of that address in a

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
				hierarchical format: *server.organization.type*. For example, www.whitehouse.gov identifies the Web serve at the White House, which is part of the U.S. government." Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 158. The following is a brief description of the substance of Dr. Jones' and/or the named inventors' testimony about the term "domain name": 1. examples of domain names as a series of characters; 2. how a domain name is used in the Internet; and 3. why a domain name corresponds either to a computer or a group of computers.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
4	**web site**	a computer associated with a domain name and that can communicate in a network	See Intrinsic Evidence for "secure web site" below. Also see: "BACKGROUND OF THE INVENTION A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet. The variety stems, in part, from the different needs of different Internet users. A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. 1. Two terminals, an originating terminal 100 and a destination terminal 110 are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping. For	See extrinsic evidence for "secure web site."

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			example, terminal 100 may transmit secret information to terminal 110 over the Internet 107. Also, it may be desired to prevent an eavesdropper from discovering that terminal 100 is in communication with terminal 110. For example, if terminal 100 is a user and terminal 110 hosts a web site, terminal 100's user may not want anyone in the intervening networks to know what web sites he is "visiting." Anonymity would thus be an issue, for example, for companies that want to keep their market research interests private and thus would prefer to prevent outsiders from knowing which web-sites or other Internet resources they are "visiting." These two security issues may be called data security and anonymity, respectively." Col. 1:14-37.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			"Data security is usually tackled using some form of data encryption. An encryption key 48 is known at both the originating and terminating terminals 100 and 110. The keys may be private and public at the originating and destination terminals 100 and 110, respectively or they may be symmetrical keys (the same key is used by both parties to encrypt and decrypt). Many encryption methods are known and usable in this context." Col. 1:37- 45. "FIG. 1 is an illustration of secure communications over the Internet according to a prior art embodiment." Col. 6:13-14. FIG. 1 Col. 37:30-39; 38:14-16; Fig. 25;	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			see also col. 19:42-44.	
5	**secure web site / secure target web site**	a computer associated with a domain name and that can communicate in a virtual private network / a target computer associated with a domain name and that can communicate in a virtual private network	See Intrinsic Evidence for "VPN," "DNS," and "web site" above. "B. Use of a DNS Proxy to Transparently Create Virtual Private Networks A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function. Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address	"TCP/IP defines the term *host computer* to refer to any computer system that connects to an internet and runs applications." Douglas E. Comer, *Computer Networks and Internets* (2d ed. 1999) p. 231. "Host: An end-user's computer connected to a network. In an internet, each *Networks and Internets* (2d ed. 1999) p. 527. "A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e. application) programs. We will follow the traditional usage and call these machines hosts." Andrew S. Tanenbaum, *Computer Networks* (3d ed. 1996) p. 11. The following is a brief description

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			that is returned to the user's browser and then used by the browser to contact the destination web site." Col. 37:17-29. "This conventional scheme is shown in FIG. 25. A user's computer 2501 includes a client application 2504 (for example, a web browser) and an IP protocol stack 2505. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack 2505) to a DNS 2502 to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application 2504, which is then able to use the IP address to communicate with the host 2503 through separate transactions such as PAGE REQ and PAGE RESP. In the conventional architecture	of the substance of Dr. Jones' and/or the named inventors' testimony about the term "secure web site": 1. why the term "secure web site" (including the term "web site") has special meaning in the context of the patented invention; 2. what makes a "web site" a computer or host in a computer network such as the Internet in the context of the patented invention; 3. examples of the various kinds of web sites in a computer network such as the Internet in the context of the patented invention; and 4. what makes a web site "secure" in a computer network such as the Internet in the context of the patented invention.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			shown in FIG. 25, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet. One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535). The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users." Col. 37:30-62. FIG. 25 (PRIOR ART) "FIG. 26 shows a system employing various principles	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			summarized above. A user's computer 2601 includes a conventional client (e.g., a web browser) 2605 and an IP protocol stack 2606 that preferably operates in accordance with an IP hopping function 2607 as outlined above. A modified DNS server 2602 includes a conventional DNS server function 2609 and a DNS proxy 2610. A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2704. An "unsecure" target site 2611 is also accessible via conventional IP protocols. According to one embodiment, DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604. In one embodiment, gatekeeper 2603 creates "hopblocks" to be used by computer 2601 and secure target site 2604 for secure communication. Then, gatekeeper 2603 communicates these to user computer 2601. Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			a secure administrative VPN. The address that is returned need not be the actual address of the destination computer. Had the user requested lookup of a nonsecure web site such as site 2611, DNS proxy would merely pass through to conventional DNS server 2609 the lookup request, which would be handled in a conventional manner, returning the IP address of non-secure web site 2611. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy 2610 would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results. Gatekeeper 2603 can be	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			implemented on a separate computer (as shown in FIG. 26) or as a function within modified DNS server 2602. In general, it is anticipated that gatekeeper 2703 facilitates the allocation and exchange of information needed to communicate securely, such as using "hopped" IP addresses. Secure hosts such as site 2604 are assumed to be equipped with a secure communication function such as an IP hopping function 2608." Col. 38:13-65. FIG. 26 "FIG. 27 shows steps that can be executed by DNS proxy server 2610 to handle requests for DNS look-up for secure hosts. In step 2701, a DNS lookup request is received for a target host. In step 2702, a check is made to determine whether access to a	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			secure host was requested. If not, then in step 2703 the DNS request is passed to conventional DNS server 2609, which looks up the IP address of the target site and returns it to the user's application for further processing. In step 2702, if access to a secure host was requested, then in step 2704 a further check is made to determine whether the user is authorized to connect to the secure host." Col. 38:66- 39:9; see also col. 39:10-25; 39:30-33; 39:61-40:13. Col. 1:38-45. FIG. 27 Claim 5.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
6	**DNS proxy server**	a computer or program that responds to a domain name inquiry in place of a DNS	See Intrinsic Evidence for "VPN", "transparently . . .," and "DNS" above. In addition: "Improvements to the basic design include … a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry …" Abstract. "Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to maintain. They can be compromised by virtual-machine applications ("applets"). They	See Extrinsic Evidence for "VPN", "transparently", and "DNS." In addition: "Proxy: An entity or device that, in the interest of efficiency, essentially stands in for another entity." Jade Clayton, McGraw-Hill Illustrated Telecom Dictionary (2nd ed. 2000) p. 470. "Proxy: An element that responds on behalf of another element to a request using a particular protocol." Frank Hargrave, Hargrave's Communications Dictionary (IEEE Press, 2001) p. 413. "Server – (1) A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T) (2) In a network, a data station that provides

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc." Col. 2:52-63. "Further improvements described in this continuation-in-part application include: … a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry …" Col. 5:65-6:3. "FIG. 26 shows a system employing a DNS proxy server with transparent VPN creation." Col. 7:19-21.	facilitates to other stations; for example, a file server, a print server, a mail server. (A) (3) In the AIX operating system, an application program that usually runs in the background and is controlled by the system program controller. (4) In AIX Enhanced X-Windows, a program that provides the basic windowing mechanism. It handles interprocess communication (IPC) connections from clients, demultiplexes graphics requests onto screens, and multiplexes input back to clients. (5) See name server. (6) In TCP/IP, a system in a network that handles the requests of a system at another site, called client-server." George McDaniel, *IBM Dictionary of Computing* (10th ed. 1993), p. 612. The following is a brief description of the substance of Dr. Jones' and/or the named inventors'

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			"The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: … a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry …" Col. 32:29-35. Fig. 26. "B. Use of a DNS Proxy to Transparently Create Virtual Private Networks A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function." Col. 37:17-21. "According to certain aspects of the invention, a specialized DNS	testimony about the term "DNS proxy server": 1. the function and operation of proxy servers outside the patented invention and in general; 2. the function and operation of conventional DNS servers; and 3. the function and operation of the DNS proxy server described in the '135 patent.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users who make an identical DNS request could be provided with different results." Col. 37:63-38:12. "FIG. 26 shows a system employing various principles summarized above. A user's computer 2601 includes a conventional client (e.g., a web browser) 2605 and an IP protocol stack 2606 that preferably operates in accordance with an IP hopping function 2607 as outlined above. A modified DNS server 2602 includes a conventional DNS server function 2609 and a DNS proxy 2610. A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2704. An	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			"unsecure" target site 2611 is also accessible via conventional IP protocols." Col. 38:13-22. "According to one embodiment, DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604. In one embodiment, gatekeeper 2603 creates "hopblocks" to be used by	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer 2601 and secure target site 2604 for secure communication. Then, gatekeeper 2603 communicates these to user computer 2601. Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer." Col. 38:23-42. "Had the user requested lookup of a non-secure web site such as site 2611, DNS proxy would merely pass through to conventional DNS server 2609 the look-up request, which would be handled in a conventional manner, returning the IP address of non-	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			secure web site 2611. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy 2610 would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results." Col. 38:43-52. "Gatekeeper 2603 can be implemented on a separate computer (as shown in FIG. 26) or as a function within modified DNS server 2602. In general, it is anticipated that gatekeeper 2703 facilitates the allocation and exchange of information needed to communicate securely, such as using "hopped" IP addresses. Secure hosts such as site 2604 are assumed to be equipped with a secure communication function	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			such as an IP hopping function 2608." Col. 38:53-60. "It will be appreciated that the functions of DNS proxy 2610 and DNS server 2609 can be combined into a single server for convenience. Moreover, although element 2602 is shown as combining the functions of two servers, the two servers can be made to operate independently." Col. 38:61-65. "FIG. 27 shows steps that can be executed by DNS proxy server 2610 to handle requests for DNS look-up for secure hosts. In step 2701, a DNS lookup request is received for a target host. In step 2702, a check is made to determine whether access to a secure host was requested. If not, then in step 2703 the DNS request is passed to conventional DNS	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			server 2609, which looks up the IP address of the target site and returns it to the user's application for further processing." Col. 38:66- 39:6. "In step 2702, if access to a secure host was requested, then in step 2704 a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper 2603 (e.g., over an "administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			requesting access must match that security level. The user's security level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges." Col. 39:7-20. "If the user is not authorized to access the secure site, then a "host unknown" message is returned (step 2705). If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			creating the secure link). As described in various embodiments of this application, any of various fields can be "hopped" (e.g., IP source/destination addresses; a field in the header; etc.) in order to communicate securely." Col. 39:21-33. Fig. 27. "Some or all of the security functions can be embedded in gatekeeper 2603, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy 2610 communicates with gatekeeper 2603 to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site. Various scenarios for implementing these features are described by way of example below:	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN. Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be received by the DNS proxy server	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			2610, which would forward the request to gatekeeper 2603. The gatekeeper would reject the request, informing DNS proxy server 2610 that it was unable to find the target computer. The DNS proxy 2610 would then return a "host unknown" error message to the client. Scenario #3: Client has permission to connect using a normal non-VPN link, and the gatekeeper does not have a rule to set up a VPN for the client to the target site. In this scenario, the client's DNS request is received by DNS proxy server 2610, which would check its rules and determine that no VPN is needed. Gatekeeper 2603 would then inform the DNS proxy server to forward the request to conventional DNS server 2609, which would resolve the request	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			and return the result to the DNS proxy server and then back to the client. Scenario #4: Client does not have permission to establish a normal/non- VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In this scenario, the DNS proxy server would receive the client's DNS request and forward it to gatekeeper 2603. Gatekeeper 2603 would determine that no special VPN was needed, but that the client is not authorized to communicate with non- VPN members. The gatekeeper would reject the request, causing DNS proxy server 2610 to return an error message to the client." Col. 39:34-40:13. Col. 38:61-65; 5:65-6:3; 32:29-	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			35; 38:66-39:1; 38:23-33; 38:43-52; 39:42- 40:13. VNET 00221425; compare VNET 00221217; also 221219, 221220, 221503-504, 505. Compare '135 patent claims 2 and 8.	
7	between the client computer and the target computer	[no construction necessary]	See Intrinsic Evidence for "target computer" below. See also: "The link key 146 is the encryption key used for encrypted communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal 100 and the destination TARP terminal 110." '135::7:61-65. "FIG. 23 shows a computer node 2301 employing various principles of the above-described embodiments. It is assumed that	"between… **1** in the space, time, etc. that separates (two things) **2** connecting *[*a bond *between* friends*]* **3** by the joint action of **4** in the combined possession of **5** from one or the other of *[*choose *between* us*]* **6** involving *[*a struggle *between* powers*]* — **adv.** in an intermediate space, time, etc." Webster's New World™ Dictionary and Thesaurus, © 1996 by Simon & Schuster, Inc., p. 57.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			two computer nodes of the type shown in FIG. 23 communicate over a plurality of separate physical transmission paths. As shown in FIG. 23 , four transmission paths X 1 through X 4 are defined for communicating between the two nodes." '135::34:53-59. "According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user." '135::37:63-38:2. "A gatekeeper server 2603 is interposed between the modified	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			DNS server and a secure target site 2704." '135::38:19-21. "If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link)." '135::39:22-29. "Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610 , which	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			would forward the request to gatekeeper 2603 . The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN." '135::39:42-52.	
8	between the client computer and the secure target computer	[no construction necessary]	See Intrinsic Evidence for "target computer" below. See also: "The link key 146 is the encryption key used for encrypted communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal 100 and the destination TARP	"between… **1** in the space, time, etc. that separates (two things) **2** connecting *[*a bond *between* friends*]* **3** by the joint action of **4** in the combined possession of **5** from one or the other of *[*choose *between* us*]* **6** involving *[*a struggle *between* powers*]* — **adv.** in an intermediate space, time, etc." Webster's New World™ Dictionary and Thesaurus, © 1996 by Simon &

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			terminal 110." '135::7:61-65. "FIG. 23 shows a computer node 2301 employing various principles of the above-described embodiments. It is assumed that two computer nodes of the type shown in FIG. 23 communicate over a plurality of separate physical transmission paths. As shown in FIG. 23 , four transmission paths X 1 through X 4 are defined for communicating between the two nodes." '135::34:53-59. "According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual	Schuster, Inc., p. 57.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			private network between the target node and the user." '135::37:63-38:2. "A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2704." '135::38:19-21. "If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link)." '135::39:22-29. "Scenario #1: Client has permission to access target	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610 , which would forward the request to gatekeeper 2603 . The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN." '135::39:42-52.	
9	between the client computer and the secure web computer	[no construction necessary]	See Intrinsic Evidence for "secure web computer" below. See also: "The link key 146 is the encryption key used for encrypted communication between the end points (TARP terminals or TARP	"between… **1** in the space, time, etc. that separates (two things) **2** connecting *[*a bond *between* friends*]* **3** by the joint action of **4** in the combined possession of **5** from one or the other of *[*choose *between* us*]* **6** involving *[*a struggle

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			routers) of a single link in the chain of hops connecting the originating TARP terminal 100 and the destination TARP terminal 110." '135::7:61-65. "FIG. 23 shows a computer node 2301 employing various principles of the above-described embodiments. It is assumed that two computer nodes of the type shown in FIG. 23 communicate over a plurality of separate physical transmission paths. As shown in FIG. 23 , four transmission paths X 1 through X 4 are defined for communicating between the two nodes." '135::34:53-59. "According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are	*between* powers*]* — **adv.** in an intermediate space, time, etc." Webster's New World™ Dictionary and Thesaurus, © 1996 by Simon & Schuster, Inc., p. 57.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user." '135::37:63-38:2. "A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2704." '135::38:19-21. "If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			creating the secure link)." '135::39:22-29. "Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610 , which would forward the request to gatekeeper 2603 . The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN." '135::39:42-52.	
10	between the client and a	[no construction necessary]	See: "The link key 146 is the encryption key used for encrypted	"between… **1** in the space, time, etc. that separates (two things) **2**

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
	second computer		communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal 100 and the destination TARP terminal 110." '135::7:61-65. "FIG. 23 shows a computer node 2301 employing various principles of the above-described embodiments. It is assumed that two computer nodes of the type shown in FIG. 23 communicate over a plurality of separate physical transmission paths. As shown in FIG. 23 , four transmission paths X 1 through X 4 are defined for communicating between the two nodes." '135::34:53-59. "According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type	connecting *[*a bond *between* friends*]* **3** by the joint action of **4** in the combined possession of **5** from one or the other of *[*choose *between* us*]* **6** involving *[*a struggle *between* powers*]* — **adv.** in an intermediate space, time, etc." Webster's New World™ Dictionary and Thesaurus, © 1996 by Simon & Schuster, Inc., p. 57.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user." '135::37:63-38:2. "A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2704." '135::38:19-21. "If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			transparently to the user (i.e., the user need not be involved in creating the secure link)." '135::39:22-29. "Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610 , which would forward the request to gatekeeper 2603 . The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN." '135::39:42-52.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
11	generating from the client computer a Domain Name Service (DNS) request	[no construction necessary]	See Intrinsic Evidence for "DNS" above.	
12	target computer	a computer with which the client computer seeks to communicate	"According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if	"**target computer**… *n.* The computer that receives data from a communications device, a hardware add-in, or a software package." Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 461.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites." '135::37:63-38:11. "According to one embodiment, DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604 . In one embodiment, gatekeeper 2603 creates "hopblocks" to be used by computer 2601 and secure target site 2604 for secure communication. Then, gatekeeper 2603 communicates these to user computer 2601 . Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer."	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			'135::38:23-40. "Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610 , which would forward the request to gatekeeper 2603 . The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN. Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			received by the DNS proxy server 2610 , which would forward the request to gatekeeper 2603 . The gatekeeper would reject the request, informing DNS proxy server 2610 that it was unable to find the target computer. The DNS proxy 2610 would then return a "host unknown" error message to the client. Scenario #3: Client has permission to connect using a normal non-VPN link, and the gatekeeper does not have a rule to set up a VPN for the client to the target site. In this scenario, the client's DNS request is received by DNS proxy server 2610 , which would check its rules and determine that no VPN is needed. Gatekeeper 2603 would then inform the DNS proxy server to forward the request to conventional DNS server 2609 ,	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			which would resolve the request and return the result to the DNS proxy server and then back to the client. Scenario #4: Client does not have permission to establish a normal/non-VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In this scenario, the DNS proxy server would receive the client's DNS request and forward it to gatekeeper 2603 . Gatekeeper 2603 would determine that no special VPN was needed, but that the client is not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing DNS proxy server 2610 to return an error message to the client." '135::39:42-40:13.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
13	virtual private link	a communication link that permits computers to privately communicate with each other by encrypting traffic on insecure communication paths between the computers	See Intrinsic Evidence for "VPN" above. See also: "As another extension to the stated architecture, multiple physical paths can be used by a client, in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. As shown in FIG. 10 , for example, client 1001 can establish three simultaneous sessions with each of three TARP routers provided by different ISPs 1011 , 1012 , 1013." '135::18:15-21. "Beginning in step 2201 , the transmission quality of a given transmission path is measured. As	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			described above, this measurement can be based on a comparison between the number of packets transmitted over a particular link to the number of packet acknowledgements received over the link (e.g., per unit time, or in absolute terms). Alternatively, the quality can be evaluated by comparing the number of packets that are acknowledged within the transmission window to the number of packets that were transmitted within that window. In yet another variation, the number of missed synchronization messages can be used to indicate link quality." '135::33:53:64. "When a packet is received from a known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,502,135				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL. The VPLs can be torn down when they become inactive for a time period, or they can be torn down upon user log-out." '135::44:39-45.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,490,151				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Support**
1	between the client and the secure server	[no construction necessary]	See same term for '135 patent.	See same term for '135 patent. *See* also: "between… **1** in the space, time, etc. that separates (two things) **2** connecting *[*a bond *between* friends*]* **3** by the joint action of **4** in the combined possession of **5** from one or the other of *[*choose *between* us*]* **6** involving *[*a struggle *between* powers*]* — **adv.** in an intermediate space, time, etc." Webster's New World™ Dictionary and Thesaurus, © 1996 by Simon & Schuster, Inc., p. 57.
2	domain name (including domain)	a name corresponding to an IP address	See same term for '135 patent.	See same term for '135 patent.
3	secure server / secure web computer	a server that requires authorization for access and that can communicate	See Intrinsic Evidence for "VPN" in '135 patent and "secure communication link" in the '504	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,490,151				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Support**
		in a secure communication link	and '211 patents. See also: "Two terminals, an originating terminal 100 and a destination terminal 110 are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping." '151::1:32-35. "In step 2702, if access to a secure host was requested, then in step 2704 a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper 2603 (e.g., over an "administrative" VPN that is	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,490,151				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Support**
			secure). It will be appreciated that different levels of security can also be provided for different categories of hosts." '151::38:44-51. "One advantage of the above-described architecture is that signaling server 3101 need only maintain a small amount of information on a large number of potential users, yet it retains the capability of quickly rejecting packets from unauthorized users such as hacker computer 3105." '151::44:61-65.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,188,180				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
1	**virtual private network (VPN)**	a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers	See Intrinsic Evidence for "virtual private network" in the '135 patent.	See Extrinsic Evidence for "virtual private network" in the '135 patent.
2	domain name (including domain)	a name corresponding to an IP address	See Intrinsic Evidence for "domain name" in the '135 patent.	See Extrinsic Evidence for "domain name" in the '135 patent.
3	domain name service (DNS)	a lookup service that returns an IP address for a requested domain name	See Intrinsic Evidence for "domain name service" in the '135 patent.	See Extrinsic Evidence for "domain name service" in the '135 patent.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
1	cryptographic information	information that is used to encode data or information that is used to decoded data	"According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon	"Cryptographic": "in an encrypted form; using a code or cipher." ACADEMIC PRESS DICTIONARY OF SCIENCE AND TECHNOLOGY 556 (1992) (second definition). "**cryptography**… *n*. The use of codes to convert data so that only a specific recipient will be able to read it, using a key. The persistent problem of cryptography is that the key must be transmitted to the intended recipient and may be intercepted. Public key cryptography is a recent significant advance." Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 124. "cryptography[:] the technology of encoding information so that it cannot be read by an unauthorized person. See ENCRYPTION and its crossreferences." *Dictionary of*

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first computer." Col. 6:37-55; see also col. 6:21-36. "FIG. 33 shows a system block diagram of a computer network in which the "one-click" secure communication link of the present invention is suitable for use." Col. 9:35-37; Fig. 33. "Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of LCGs. This vulnerability can be mitigated by incorporating an encryptor, designed to scramble the output as part of the random number	*Computer and Internet Terms* 111 (6th ed. 1998) Dr. Mark Jones, a professor of Electrical and Computer Engineering at Virginia Tech, may offer expert testimony regarding the view of one of ordinary skill in the art as of the filing date of the '759 patent. The following is a brief description of the substance of Dr. Jones' and/or the named inventors' testimony about the term "cryptographic information": 1. examples of cryptographic information in the context of the patented invention, including but not limited to types of information that are used to encode and decode data; 2. how information is used to encode and decode data in the

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			generator. The random number generator prevents an adversary from mounting an attack--e.g., a known plaintext attack--against the encryptor." Col. 31:21-28. "According to one inventive improvement, a "link guard" function 2805 is inserted into the highbandwidth node (e.g., ISP 2803) that quickly discards packets destined for a low-bandwidth target node if they are not valid packets. Each packet destined for a low-bandwidth node is cryptographically authenticated to determine whether it belongs to a VPN. If it is not a valid VPN packet, the packet is discarded at the highbandwidth node. If the packet is authenticated as belonging to a VPN, the packet is passed with high preference. If the packet is a	context of the patented invention; and 3. how secure communication modes of communication are enabled without a user having to enter cryptographic information in the patented inventions.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			valid non- VPN packet, it is passed with a lower quality of service (e.g., lower priority)." Col. 43:29-41. "One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535)." Col. 40:24-33. "FIG. 27 shows steps that can be executed by DNS proxy server	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			2610 to handle requests for DNS look-up for secure hosts. In step 2701, a DNS look- up request is received for a target host. In step 2702, a check is made to determine whether access to a secure host was requested. If not, then in step 2703 the DNS request is passed to conventional DNS server 2609, which looks up the IP address of the target site and returns it to the user's application for further processing. In step 2702, if access to a secure host was requested, then in step 2704 a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper 2603 (e.g., over an	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			"administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user's security level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges. If the user is not authorized to access the secure site, then a "host unknown" message is returned (step 2705). If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link)." Col. 41:43-42:6. "According to one embodiment of the improvement, ISP 2901 maintains a separate VPN with first host computer 2900, and thus translates packets arriving at the ISP into packets having a different IP header before they are transmitted to host computer 2900. The cryptographic keys used to authenticate VPN packets at the link guard 2911 and the cryptographic keys used to encrypt and decrypt the VPN packets at host 2902 and host 2901 can be different, so that link	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			guard 2911 does not have access to the private host data; it only has the capability to authenticate those packets." Col. 44:41-51. "F. One-Click Secure On-Line Communications and Secure Domain Name Service The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer (i.e., no click). FIG. 33 shows a system block diagram 3300 of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. 33, a computer terminal or client computer 3301, such as a personal computer (PC), is connected to a computer network 3302, such as the Internet, through an ISP 3303. Alternatively, computer 3301 can be connected to computer network 3302 through an edge router. Computer 3301 includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer 3301 can communicate conventionally with another computer 3304 connected to computer network 3302 over a communication link 3305 using a browser 3306 that is installed and	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			operates on computer 3301 in a wellknown manner." Col. 50:19-44. "FIG. 34 shows a flow diagram 3400 for installing and establishing a "oneclick" secure communication link over a computer network according to the present invention. At step 3401, computer 3301 is connected to server computer 3304 over a non-VPN communication link 3305. Web browser 3306 displays a web page associated with server 3304 in a well-known manner. According to one variation of the invention, the display of computer 3301 contains a hyperlink, or an icon representing a hyperlink, for selecting a virtual private network (VPN) communication link ("go secure" hyperlink) through computer network 3302 between terminal 3301 and server 3304.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			Preferably, the "go secure" hyperlink is displayed as part of the web page downloaded from server computer 3304, thereby indicating that the entity providing server 3304 also provides VPN capability. By displaying the "go secure" hyperlink, a user at computer 3301 is informed that the current communication link between computer 3301 and server computer 3304 is a non-secure, non-VPN communication link. At step 3402, it is determined whether a user of computer 3301 has selected the "go secure" hyperlink. If not, processing resumes using a nonsecure (conventional) communication method (not shown). If, at step 3402, it is determined that the user has selected the "go secure" hyperlink, flow continues to step 3403 where an object associated	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			with the hyperlink determines whether a VPN communication software module has already been installed on computer 3301." 50:50-51:8. "By clicking on the "go secure" hyperlink, a user at computer 3301 has enabled a secure communication mode of communication between computer 3301 and server computer 3304. According to one variation of the invention, the user is not required to do anything more than merely click the "go secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer 3301 and server computer 3304 are performed transparently to a user at computer 3301. At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link." 51:34-47. "Alternatively, SDNS 3313 can be accessed through secure portal 3310 "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal 3310 preferably authenticates the query using any well-known technique, such as a cryptographic technique; before allowing the query to proceed to SDNS 3319. Because the initial communication link in this situation is not a VPN communication link, the reply to	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			the query can be "in the clear." The querying computer can use the clear reply for establishing a VPN link to the desired domain name. Alternatively, the query to SDNS 3313 can be in the clear, and SDNS 3313 and gatekeeper 3314 can operate to establish a VPN communication link to the querying computer for sending the reply." Col. 53:3-16; see also 52:33-55. "When software module 3309 is being installed or when the user is off-line, the user can optionally specify that all communication links established over computer network 3302 are secure communication links. Thus, anytime that a communication link is established, the link is a VPN link. Consequently, software module 3309 transparently	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			accesses SDNS 3313 for obtaining the URL for a selected secure website. In other words, in one embodiment, the user need not "click" on the secure option each time secure communication is to be effected." Col. 53:38-47. "Additionally, a user at computer 3301 can optionally select a secure communication link through proxy computer 3315. Accordingly, computer 3301 can establish a VPN communication link 3323 with secure server computer 3320 through proxy computer 3315. Alternatively, computer 3301 can establish a non-VPN communication link 3324 to a nonsecure website, such as non-secure server computer 3304." Col. 53:48-52; see also col. 52:12-29. Also see Notice of Allowability, p. 2	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			(VNET00009711) ("The prior arts [sic] of record do not teach a system and a method for establishing a secure communication link being a virtual private network communication link between a client computer and a server computer over a computer network. The secure communication link is established based on secure communication mode that is enable [sic] at the first computer without a user entering any cryptographic information for establishing the secure communication mode of communication."). VNET 00220050.	
2	enabling/enable a secure communication	[no construction necessary]	"According to one aspect of the present invention, a user can conveniently establish a VPN	"**enable**… *vb*. To activate or turn on." Microsoft Press, Computer

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
	mode of communication		using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first	Dictionary (3rd ed. 1997), p. 175. "enable - 1 a: provide with the means or opportunity, training that ~s people to earn a living> b: to to make possible, practical, or easy c: to cause to operate (software that ~s the keyboard>" *Merriam-Webster's Collegiate Dictionary* 379, 591 (10th ed. 2002). The following is a brief description of the substance of Dr. Jones' and/or the named inventors' testimony about the term "enabling a secure communication mode of communication": 1. secure communication in the context of the patented inventions, including but not limited to manners in which a secure communication mode of communication is enabled; 2. how communications are

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication software module when the software module is not stored on the first computer. Subsequently, the proxy software module is stored in the first computer." Col. 6:36-63. "F. One-Click Secure On-Line Communications and Secure	made secure and how security is enabled in the context of the patented invention; and 3. the role of the user in enabling a secure communication mode of communication.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			Domain Name Service The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. 33 shows a system block diagram 3300 of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. 33, a computer terminal or client computer 3301, such as a	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			personal computer (PC), is connected to a computer network 3302, such as the Internet, through an ISP 3303. Alternatively, computer 3301 can be connected to computer network 3302 through an edge router. Computer 3301 includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer 3301 can communicate conventionally with another computer 3304 connected to computer network 3302 over a communication link 3305 using a browser 3306 that is installed and operates on computer 3301 in a well-known manner." Col. 50:19-44. "Flow continues to step 3405 where, after computer 3301 connects to website 3308, the software module for establishing	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			a communication link is downloaded and installed in a well-known manner on computer terminal 3301 as software module 3309. At step 3405, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over computer network 3302. At step 3406, the -communication link between computer 3301 and website 3308 is then terminated in a well-known manner. By clicking on the "go secure" hyperlink, a user at computer 3301 has enabled a secure communication mode of communication between computer 3301 and server computer 3304. According to one variation of the invention, the user is not required to do anything more than merely click the "go	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between computer 3301 and server computer 3304 are performed transparently to a user at computer 3301. At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link. In one embodiment, software module 3309 automatically replaces the top-level domain name for server 3304 within browser 3406 with a secure top-level domain name for server computer 3304. For example, if	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			the top-level domain name for server 3304 is .com, software module 3309 replaces the .com top-level domain name with a .scom top-level domain name, where the "s" stands for secure. Alternatively, software module 3409 can replace the top-level domain name of server 3304 with any other non-standard top-level domain name." Col. 51:23-57. "Flow continues to step 3405 where, after computer 3301 connects to website 3308, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal 3301 as software module 3309. At step 3405, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			all communication links over computer network 3302. At step 3406, the -communication link between computer 3301 and website 3308 is then terminated in a well-known manner. By clicking on the "go secure" hyperlink, a user at computer 3301 has enabled a secure communication mode of communication between computer 3301 and server computer 3304. According to one variation of the invention, the user is not required to do anything more than merely click the "go secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer 3301 and server computer 3304 are performed transparently to a user at computer 3301. At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link. In one embodiment, software module 3309 automatically replaces the top-level domain name for server 3304 within browser 3406 with a secure top-level domain name for server computer 3304. For example, if the top-level domain name for server 3304 is .com, software module 3309 replaces the .com top-level domain name with a .scom top-level domain name, where the "s" stands for secure. Alternatively, software module 3409 can replace the top-level domain name of server 3304 with	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			any other non-standard top-level domain name." Col. 39:57-40:55. FIG. 26 FIG. 33 FIG. 34	
3	virtual private network	a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers	*See* intrinsic evidence for '135 Patent "VPN."	*See* extrinsic evidence for '135 Patent "VPN."
4	between the first computer and a second computer	[no construction necessary]	"According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a	*See* extrinsic evidence for '135 patent "between…" "between… **1** in the space, time, etc. that separates (two things) **2** connecting *[*a bond *between* friends*]* **3** by the joint action of **4** in the combined possession of **5**

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled	from one or the other of *[*choose *between* us*]* **6** involving *[*a struggle *between* powers*]* — **adv.** in an intermediate space, time, etc." Webster's New World™ Dictionary and Thesaurus, © 1996 by Simon & Schuster, Inc., p. 57.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication software module when the software module is not stored on the first computer. Subsequently, the proxy software module is stored in the first computer." Col. 6:36-63. "F. One-Click Secure On-Line Communications and Secure Domain Name Service The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. 33 shows a system block diagram 3300 of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. 33, a computer terminal or client computer 3301, such as a personal computer (PC), is connected to a computer network 3302, such as the Internet, through an ISP 3303. Alternatively, computer 3301 can be connected to computer	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			network 3302 through an edge router. Computer 3301 includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer 3301 can communicate conventionally with another computer 3304 connected to computer network 3302 over a communication link 3305 using a browser 3306 that is installed and operates on computer 3301 in a well-known manner. Computer 3304 can be, for example, a server computer that is used for conducting e-commerce. In the situation when computer network 3302 is the Internet, computer 3304 typically will have a standard top-level domain name such as .com, .net, .org, .edu, .mil or .gov. FIG. 34 shows a flow diagram 3400 for installing and establishing a "one-click" secure	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			communication link over a computer network according to the present invention. At step 3401, computer 3301 is connected to server computer 3304 over a non-VPN communication link 3305. Web browser 3306 displays a web page associated with server 3304 in a well-known manner. According to one variation of the invention, the display of computer 3301 contains a hyperlink, or an icon representing a hyperlink, for selecting a virtual private network (VPN) communication link ("go secure" hyperlink) through computer network 3302 between terminal 3301 and server 3304. Preferably, the "go secure" hyperlink is displayed as part of the web page downloaded from server computer 3304, thereby indicating that the entity providing server 3304 also provides VPN capability." Col.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			50:19-64. "Flow continues to step 3405 where, after computer 3301 connects to website 3308, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal 3301 as software module 3309. At step 3405, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over computer network 3302. At step 3406, the -communication link between computer 3301 and website 3308 is then terminated in a well-known manner. By clicking on the "go secure" hyperlink, a user at computer 3301 has enabled a secure communication mode of communication between	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer 3301 and server computer 3304. According to one variation of the invention, the user is not required to do anything more than merely click the "go secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between computer 3301 and server computer 3304 are performed transparently to a user at computer 3301. At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link. In one embodiment, software module 3309 automatically	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			replaces the top-level domain name for server 3304 within browser 3406 with a secure top-level domain name for server computer 3304. For example, if the top-level domain name for server 3304 is .com, software module 3309 replaces the .com top-level domain name with a .scom top-level domain name, where the "s" stands for secure. Alternatively, software module 3409 can replace the top-level domain name of server 3304 with any other non-standard top-level domain name." Col. 51:23-57. "Flow continues to step 3405 where, after computer 3301 connects to website 3308, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal 3301 as software module 3309. At step 3405, a user can	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over computer network 3302. At step 3406, the -communication link between computer 3301 and website 3308 is then terminated in a well-known manner. By clicking on the "go secure" hyperlink, a user at computer 3301 has enabled a secure communication mode of communication between computer 3301 and server computer 3304. According to one variation of the invention, the user is not required to do anything more than merely click the "go secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			communication link. All procedures required for establishing a secure communication link between computer 3301 and server computer 3304 are performed transparently to a user at computer 3301. At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link. In one embodiment, software module 3309 automatically replaces the top-level domain name for server 3304 within browser 3406 with a secure top-level domain name for server computer 3304. For example, if the top-level domain name for server 3304 is .com, software module 3309 replaces the .com top-level domain name with a .scom top-level domain name,	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 6,839,759				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			where the "s" stands for secure. Alternatively, software module 3409 can replace the top-level domain name of server 3304 with any other non-standard top-level domain name." Col. 39:57-40:55. FIG. 33 FIG. 34 *See also* intrinsic evidence for '135 patent "between…"	
5	secure communication link	an encrypted communication link	*See* intrinsic evidence for '504 patent "secure communication link".	*See* extrinsic evidence for '504 patent "secure communication link".

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
1	**Domain Name Service (DNS)**	a lookup service that returns an IP address for a requested domain name	*See* intrinsic evidence for '135 Patent "DNS"; *see also* intrinsic evidence for '504 patent "an indication that the domain name service system supports establishing a secure communication link"	*See* extrinsic evidence for '135 Patent "DNS"
2	**domain name**	a name corresponding to an IP address	*See* intrinsic evidence for '135 Patent "domain name"	*See* extrinsic evidence for '135 Patent "domain name"
3	domain name service system	a computer system that includes a domain name service (DNS)	*See* intrinsic evidence for '135 Patent "domain name service" and intrinsic evidence for '504 Patent "an indication that the domain name service system supports establishing a secure communication link"	*See* extrinsic evidence for '135 Patent "domain name service" "**DNS**… *n.* **1.** Acronym for **D**omain **N**ame **S**ystem. The system by which hosts on the Internet have both domain name addresses (such as bluestem.prairienet.org) and IP addresses (such as 192.17.3.4). The domain name address is used by human users and is automatically translated into the numerical IP address, which is used by the

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
				packet-routing software. *See also* domain name address, IP address. **2.** Acronym for **D**omain **N**ame **S**ervice. The Internet utility that implements the Domain Name System (see definition 1). DNS servers, also called *name servers*, maintain databases containing the addresses and are accessed transparently to the user." Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 155 "**DNS server**… *n.* A computer that can answer Domain Name Service (DNS) queries. The DNS server keeps a database of host computers and their corresponding IP addresses. Presented with the name apex.com, for example, the DNS server would return the IP address of the hypothetical company Apex. *See also* DNS (definition 2), IP address. Microsoft Press, Computer

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
				Dictionary (3rd ed. 1997), p. 155
4	secure communication link	an encrypted communication link	"According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon	"**secure channel**… *n.* A communications link that has been protected against unauthorized access, operation, or use by means of isolation from the public network, encryption, or other forms of control. *See also* encryption." Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 425. Dr. Mark Jones, a professor of Electrical and Computer Engineering at Virginia Tech, may offer expert testimony regarding the view of one of ordinary skill in the art as of the filing date of the '504 patent. The following is a brief description of the substance of Dr. Jones' and/or the named inventors'

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication software module when the software module is not stored on the first computer. Subsequently, the proxy software	testimony about the term "secure communication link": 1. secure communication links in the context of the patented invention and 2. what one of skill in the art would understand to be a communication link and how the communication link may be secured in the context of the patents.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			module is stored in the first computer. The secure communication link is a virtual private network communication link over the computer network. Preferably, the virtual private network can be based on inserting into each data packet one or more data values that vary according to a pseudo-random sequence. Alternatively, the virtual private network can be based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses or other data values in packets transmitted between the first computer and the second computer, such that the second computer compares the data values in each data packet transmitted between the first computer and the second computer to a moving window of	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			valid values. Yet another alternative provides that the virtual private network can be based on a comparison between a discriminator field in each data packet to a table of valid discriminator fields maintained for the first computer." Col. 6:36-7:10. FIG. 33 FIG. 34 "The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. 33 shows a system block diagram 3300 of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. 33, a computer terminal or client computer 3301, such as a personal computer (PC), is connected to a computer network 3302, such as the Internet, through an ISP 3303. Alternatively, computer 3301 can be connected to computer network 3302 through an edge router. Computer 3301 includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer 3301 can communicate	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			conventionally with another computer 3304 connected to computer network 3302 over a communication link 3305 using a browser 3306 that is installed and operates on computer 3301 in a well-known manner." Col. 49:4-25. "By displaying the 'go secure' hyperlink, a user at computer 3301 is informed that the current communication link between computer 3301 and server computer 3304 is a non-secure, non-VPN communication link. At step 3402, it is determined whether a user of computer 3301 has selected the 'go secure' hyperlink. If not, processing resumes using a non-secure (conventional) communication method (not shown). If, at step 3402, it is determined that the user has selected the 'go secure'	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			hyperlink, flow continues to step 3403 where an object associated with the hyperlink determines whether a VPN communication software module has already been installed on computer 3301. Alternatively, a user can enter a command into computer 3301 to 'go secure.' If, at step 3403, the object determines that the software module has been installed, flow continues to step 3407. If, at step 3403, the object determines that the software module has not been installed, flow continues to step 3404 where a non-VPN communication link 3307 is launched between computer 3301 and a website 3308 over computer network 3302 in a well-known manner. Website 3308 is accessible by all computer terminals connected to computer network 3302 through a non-VPN	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			communication link. Once connected to website 3308, a software module for establishing a secure communication link over computer network 3302 can be downloaded and installed. Flow continues to step 3405 where, after computer 3301 connects to website 3308, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal 3301 as software module 3309. At step 3405, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over computer network 3302. At step 3406, the communication link between computer 3301 and website 3308 is then terminated in a well-known manner.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			By clicking on the 'go secure' hyperlink, a user at computer 3301 has enabled a secure communication mode of communication between computer 3301 and server computer 3304. According to one variation of the invention, the user is not required to do anything more than merely click the 'go secure' hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between computer 3301 and server computer 3304 are performed transparently to a user at computer 3301." Col. 49:46-50:24.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			VNET221020 *See also* the file history of the '504 patent, reasons for allowance: "The prior arts of record do not teach or [sic] a domain name service system configured to be connected to a communication network, to store a plurality of domain names and corresponding network addresses, to receive a query for a network address, and to comprise an indication that the domain name service system supports establishing a secure communication link."	
5	an indication that the domain name service system supports establishing a	[no construction necessary]	"That is, instead of indicating a final destination in the destination field of the IP header, the TARP packet's IP header always points to a next-hop in a series of TARP router hops, or to the final	indicate - a.: to point out or point to b: to be a sign, symptom, or index of <the high fever ~s a serious condition) c: to demonstrate or suggest the necessity or advisability of <indicated the need for a new

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
	secure communication link		destination. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be next-hop TARP router as well as the final destination." Col. 3:26-33. "1. A window sequence number--an identifier that indicates where the packet belongs in the original message sequence. 2. An interleave sequence number--an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window. 3. A time-to-live (TTL) datum--indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a datum	school) 2: to state or express briefly <indicated a desire to cooperate)" *Merriam-Webster's Collegiate Dictionary* 591 (10th ed. 2002). The following is a brief description of the substance of Dr. Jones' and/or the named inventors' testimony about the term "an indication that the domain name service system supports establishing a secure communication link": 1. how the domain name service system of the patents comprises an indication that it supports establishing a secure communication link (or indicates, in the context of the '211 patent) and 2. how establishment of a secure communication link may be supported in the context of the

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop. 4. Data type identifier--indicates whether the payload contains, for example, TCP or UDP data. 5. Sender's address--indicates the sender's address in the TARP network. 6. Destination address--indicates the destination terminal's address in the TARP network. 7. Decoy/Real--an indicator of whether the packet contains real message data or dummy decoy data or a combination." Col. 11:45-67. "S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message." Col. 15:1-3.	patented inventions.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			"At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link. In one embodiment, software module 3309 automatically replaces the top-level domain name for server 3304 within browser 3406 with a secure top-level domain name for server computer 3304. For example, if the top-level domain name for server 3304 is .com, software module 3309 replaces the .com top-level domain name with a scom top-level domain name, where the "s" stands for secure. Alternatively, software module 3409 can replace the top-level domain name of server 3304 with any other non-standard top-level domain name. Because the secure top-level domain name is a non-standard	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown. According to the invention, software module 3309 contains the URL for querying a secure domain name service (SDNS) for obtaining the URL for a secure top-level domain name. In this regard, software module 3309 accesses a secure portal 3310 that interfaces a secure network 3311 to computer network 3302. Secure network 3311 includes an internal router 3312, a secure domain name service (SDNS) 3313, a VPN gatekeeper 3314 and a secure proxy 3315. The secure network can include other network services, such as e-mail 3316, a plurality of chatrooms (of which only one chatroom 3317 is	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			shown), and a standard domain name service (STD DNS) 3318. Of course, secure network 3311 can include other resources and services that are not shown in FIG. 33. When software module 3309 replaces the standard top-level domain name for server 3304 with the secure top-level domain name, software module 3309 sends a query to SDNS 3313 at step 3408 through secure portal 3310 preferably using an administrative VPN communication link 3319. In this configuration, secure portal 3310 can only be accessed using a VPN communication link." Col. 50:25-60. "The present invention provides a technique for establishing a secure communication link between a first computer and a	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. 33 shows a system block diagram 3300 of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. 33, a computer terminal or client computer 3301, such as a personal computer (PC), is connected to a computer network 3302, such as the Internet, through an ISP 3303. Alternatively, computer 3301 can	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			be connected to computer network 3302 through an edge router. Computer 3301 includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer 3301 can communicate conventionally with another computer 3304 connected to computer network 3302 over a communication link 3305 using a browser 3306 that is installed and operates on computer 3301 in a well-known manner." Col. 49:4-25. "SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name. An entity can register a secure	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			domain name in SDNS 3313 so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website. Moreover, an entity can register several secure domain names, with each respective secure domain name representing a different priority level of access in a hierarchy of access levels to a secure website. For example, a securities trading website can provide users secure access so that a denial of service attack on the website will be ineffectual with respect to users subscribing to the secure website service. Different levels of subscription can be arranged based on, for example, an escalating fee, so that a user can select a desired level of guarantee for connecting to the secure	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			securities trading website. When a user queries SDNS 3313 for the secure computer network address for the securities trading website, SDNS 3313 determines the particular secure computer network address based on the user's identity and the user's subscription level. At step 3409, SDNS 3313 accesses VPN gatekeeper 3314 for establishing a VPN communication link between software module 3309 and secure server 3320. Server 3320 can only be accessed through a VPN communication link. VPN gatekeeper 3314 provisions computer 3301 and secure web server computer 3320, or a secure edge router for server computer 3320, thereby creating the VPN. Secure server computer 3320 can be a separate server computer from server computer 3304, or	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			can be the same server computer having both non-VPN and VPN communication link capability, such as shown by server computer 3322. Returning to FIG. 34, in step 3410, SDNS 3313 returns a secure URL to software module 3309 for the .scom server address for a secure server 3320 corresponding to server 3304. Alternatively, SDNS 3313 can be accessed through secure portal 3310 "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal 3310 preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS 3319. Because the initial communication link in this situation is not a VPN communication link, the reply to	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			the query can be "in the clear." The querying computer can use the clear reply for establishing a VPN link to the desired domain name. Alternatively, the query to SDNS 3313 can be in the clear, and SDNS 3313 and gatekeeper 3314 can operate to establish a VPN communication link to the querying computer for sending the reply." Col. 50:11-60. FIG. 33 "The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is built on top of the existing Internet protocol (IP). The secure virtual Internet works over the existing Internet infrastructure, and interfaces with client applications the same way as the existing	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			Internet. The key technologies provided by the present invention that support the secure virtual Internet include a "one-click" and "no-click" technique to become part of the secure virtual Internet, a secure domain name service (SDNS) for the secure virtual Internet, and a new approach for interfacing specific client applications onto the secure virtual Internet. According to the invention, the secure domain name service interfaces with existing applications, in addition to providing a way to register and serve domain names and addresses." Col. 6:21-35. "According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			who make an identical DNS request could be provided with different results." Col. 39:46-62. "In step 2702, if access to a secure host was requested, then in step 2704 a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper 2603 (e.g., over an "administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user's security	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges. If the user is not authorized to access the secure site, then a "host unknown" message is returned (step 2705). If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link). As described in various embodiments of this application, any of various fields can be "hopped" (e.g., IP	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			source/destination addresses; a field in the header; etc.) in order to communicate securely." Col. 40:57-41:15. *See also* the file history of the '504 patent, reasons for allowance: "The prior arts of record do not teach or [sic] a domain name service system configured to be connected to a communication network, to store a plurality of domain names and corresponding network addresses, to receive a query for a network address, and to comprise an indication that the domain name service system supports establishing a secure communication link."	
6	between a/the first location and a/the	[no construction necessary]	"According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-	*See* extrinsic evidence for '135 patent "between…" "between… **1** in the space, time,

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
	second location		click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first	etc. that separates (two things) **2** connecting *[*a bond *between* friends*]* **3** by the joint action of **4** in the combined possession of **5** from one or the other of *[*choose *between* us*]* **6** involving *[*a struggle *between* powers*]* — **adv.** in an intermediate space, time, etc." Webster's New World™ Dictionary and Thesaurus, © 1996 by Simon & Schuster, Inc., p. 57.

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication software module when the software module is not stored on the first computer. Subsequently, the proxy software module is stored in the first computer. The secure communication link is a virtual private network communication link over the computer network.	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			Preferably, the virtual private network can be based on inserting into each data packet one or more data values that vary according to a pseudo-random sequence. Alternatively, the virtual private network can be based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses or other data values in packets transmitted between the first computer and the second computer, such that the second computer compares the data values in each data packet transmitted between the first computer and the second computer to a moving window of valid values. Yet another alternative provides that the virtual private network can be based on a comparison between a discriminator field in each data	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			packet to a table of valid discriminator fields maintained for the first computer." Col. 6:36-7:10. FIG. 33 FIG. 34 "The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer (i.e., no click). FIG. 33 shows a system block diagram 3300 of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. 33, a computer terminal or client computer 3301, such as a personal computer (PC), is connected to a computer network 3302, such as the Internet, through an ISP 3303. Alternatively, computer 3301 can be connected to computer network 3302 through an edge router. Computer 3301 includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer 3301 can communicate conventionally with another computer 3304 connected to computer network 3302 over a communication link 3305 using a browser 3306 that is installed and	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			operates on computer 3301 in a well-known manner." Col. 49:4-25. "By displaying the 'go secure' hyperlink, a user at computer 3301 is informed that the current communication link between computer 3301 and server computer 3304 is a non-secure, non-VPN communication link. At step 3402, it is determined whether a user of computer 3301 has selected the 'go secure' hyperlink. If not, processing resumes using a non-secure (conventional) communication method (not shown). If, at step 3402, it is determined that the user has selected the 'go secure' hyperlink, flow continues to step 3403 where an object associated with the hyperlink determines whether a VPN communication software module has already been	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			installed on computer 3301. Alternatively, a user can enter a command into computer 3301 to 'go secure.' If, at step 3403, the object determines that the software module has been installed, flow continues to step 3407. If, at step 3403, the object determines that the software module has not been installed, flow continues to step 3404 where a non-VPN communication link 3307 is launched between computer 3301 and a website 3308 over computer network 3302 in a well-known manner. Website 3308 is accessible by all computer terminals connected to computer network 3302 through a non-VPN communication link. Once connected to website 3308, a software module for establishing a secure communication link over computer network 3302 can be	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			downloaded and installed. Flow continues to step 3405 where, after computer 3301 connects to website 3308, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal 3301 as software module 3309. At step 3405, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over computer network 3302. At step 3406, the communication link between computer 3301 and website 3308 is then terminated in a well-known manner. By clicking on the 'go secure' hyperlink, a user at computer 3301 has enabled a secure communication mode of communication between	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			computer 3301 and server computer 3304. According to one variation of the invention, the user is not required to do anything more than merely click the 'go secure' hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between computer 3301 and server computer 3304 are performed transparently to a user at computer 3301. At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link. In one embodiment, software module 3309	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,418,504				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
			automatically replaces the top-level domain name for server 3304 within browser 3406 with a secure top-level domain name for server computer 3304. For example, if the top-level domain name for server 3304 is .com, software module 3309 replaces the .com top-level domain name with a scom top-level domain name, where the 's' stands for secure. Alternatively, software module 3409 can replace the top-level domain name of server 3304 with any other non-standard top-level domain name." Col. 49:46-50:36. *See also* intrinsic evidence for '135 patent "between…"	

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,921,211				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
1	**Domain Name Service (DNS)**	a lookup service that returns an IP address for a requested domain name	*See* intrinsic evidence for '135 Patent "DNS"; see also intrinsic evidence for '504 patent "an indication that the domain name service system supports establishing a secure communication link"	*See* extrinsic evidence for '135 Patent "DNS" Dr. Mark Jones, a professor of Electrical and Computer Engineering at Virginia Tech, may offer expert testimony regarding the view of one of ordinary skill in the art as of the filing date of the '211 patent.
2	**domain name**	a name corresponding to an IP address	*See* intrinsic evidence for '135 Patent "domain name"	*See* extrinsic evidence for '135 Patent "domain name"
3	domain name service system	a computer system that includes a domain name service (DNS)	*See* intrinsic evidence for '135 Patent "domain name service" and '504 Patent "an indication that the domain name service system supports establishing a secure communication link"	*See* extrinsic evidence for '135 Patent "domain name service"
4	indicate/indicating . . . whether the domain name	[no construction necessary]	*See* intrinsic evidence for '504 Patent, "an indication that the domain name service system	*See* extrinsic evidence for '504 Patent "an indication…"

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,921,211				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
	service system supports establishing a secure communication link		supports establishing a secure communication link"	
5	secure communication link	an encrypted communication link	*See* intrinsic evidence for '504 Patent "secure communication link"	*See* extrinsic evidence for '504 Patent "secure communication link"
6	between a/the first location and a/the second location	[no construction necessary]	*See* intrinsic evidence for '504 patent "between a/the first location and a/the second location"	*See* extrinsic evidence for '504 patent "between a/the first location and a/the second location" *See* also: "between… **1** in the space, time, etc. that separates (two things) **2** connecting *[*a bond *between* friends*]* **3** by the joint action of **4** in the combined possession of **5** from one or the other of *[*choose *between* us*]* **6** involving *[*a struggle *between* powers*]* — **adv.** in an intermediate space, time, etc." Webster's New World™ Dictionary and Thesaurus,

EXHIBIT C

VirnetX's Proposed Construction of Claim Terms and Supporting Evidence

U.S. Patent No. 7,921,211				
Term #	**Claim Term/Phrase**	**VirnetX's Proposed Construction**	**Intrinsic Evidence**	**Extrinsic Evidence**
				© 1996 by Simon & Schuster, Inc., p. 57.